White Paper

Determining the Appropriate Evaluation Assurance Level for COTS IA and IA-Enabled Products

Presented by

DISA FSO GO434
IA Awareness and Training Products

March 15, 2004

Determining the Appropriate Evaluation Assurance Level for COTS IA and IA-Enabled Products

Table of Contents

Introduction

In the past, under the guidance of DoD Directive 5200.28, most DoD information systems were built to custom specifications and information assurance (IA) was primarily applied to these individual systems through a rigorous engineering process. The DoD guidance focused on making security an inherent feature of system design and establishing a trusted computing base.

Today, much of the DoD-wide network infrastructure is assembled from general-purpose, commercially designed and developed information technology (IT). Information assurance emphasis is shifting from achieving a trusted environment to knowing how to operate in an essentially unbounded and untrusted environment using a "layered protection" approach.

DoD Directive 8500.1, "Information Assurance (IA)," published on October 24, 2002, cancelled DoDD 5200.28. The intent, under the DoDD 8500.1, is to help move the DoD IA program toward netcentricity by adopting a defense-in-depth approach. Defense-in-depth calls for layering both technical and non-technical solutions throughout each DoD information system and the DoD wide infrastructure.

The use of information assurance (IA) and information assurance-enabled (IA-enabled) validated products is a part of defense-in-depth, moving away from trusted systems and toward netcentricity, and operating with assurance in an untrusted environment.

The intent of this paper is to assist in clarifying guidance on determining the required evaluation assurance level (EAL) of potential security mechanisms; specifically, commercial-off-the-shelf (COTS) IA or IA-enabled products appropriate for the DoD system in which they are to be implemented.

Robustness and Evaluation Assurance Level (EAL)

When using DoD's new IA guidelines, robustness of an IA security mechanism or an IA solution is linked to the Mission Assurance Category (MAC) of the information system in which the mechanism is going to be implemented. Robustness, in part, defines the level of assurance an IA mechanism should provide. The level of confidence and integrity/availability required of each IA solution is driven by the value of the information the system is protecting and the threat to that system. To accomplish this, each component within the system needs to provide an appropriate level of robustness.

Robustness, in the context of DoD information assurance, is defined in DoD Directive 8500.1, "Information Assurance (IA)," paragraphs E2.1.37 through E2.1.37.3, and DoD Instruction 8500.2, "Information Assurance (IA) Implementation," dated February 6, 2003, paragraphs E2.1.47 through E2.1.47.3. Implementation of robustness is described in DoDI 8500.2 paragraphs E3.2.4.3 through E3.2.4.3.5 DoDI 8500.2. Further, the three levels of robustness are discussed in detail in Chapter 4 of the "Information Assurance Technical Framework (IATF)," published by the National Security Agency (NSA), current release (Release 3.1, dated September 2002) or later.

The IA controls, as listed in attachments 1-6 of Appendix 4 to DoDI 8500.2, delineate the robustness required by a control. The IA controls describe the technical or environmental countermeasures required to meet the robustness level of the control for the Mission Assurance Category (MAC) assigned to the system. Basically, the evaluation assurance level (EAL) is related to the MAC assigned to the DoD information system and the robustness mandated in the IA controls required to meet the MAC of the system.

Robustness, as applied to the IA or IA-enabled product's EAL, cannot always be easily determined. Under most conditions, the appropriate IA controls found in attachments 1 – 6 of DoDI 8500.2 specify the robustness of the control and refer to the IATF for guidance on robustness as it relates to assurance levels.

Guidance on the technical requirements for robustness and its relationship to EAL is

found in Appendix E of the IATF, where it states, "According to the Office of the Secretary of Defense (OSD) Global Information Grid (GIG) policy, technical information assurance (IA) solutions in the defense-in-depth strategy will be at one of three defined levels of robustness: high, medium, or basic, corresponding to the level of concern assigned to the system. The three levels of technical robustness solutions identified in the OSD GIG Policy are described in the following subparagraphs."

The subparagraph for high robustness specifies, "High-assurance security design, such as specified by NSA or the International Common Criteria (CC) [requires], at a minimum, an Evaluated Assurance Level (EAL) greater than 4," and that the products be evaluated and certified by NSA.

The medium robustness subparagraph states, "Good assurance security design, such as specified in CC as EAL3 or greater," and requires that the solutions be evaluated and validated under the Common Criteria evaluation validation scheme or NSA.

The subparagraph for basic robustness indicates the assurance requirement is "CC EAL 1 or greater assurance." and that solutions are to be evaluated and validated under the National Information Assurance Partnership (NIAP) CC evaluation validation scheme or NSA.

For those systems which fall under the guidance provided by the Chairman of the Joints Chief of Staff, the CJSCM 6510.01, "Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)," dated March 25, 2003, in appendix H, enclosure C, paragraph 2b, 2c, and 2d, reiterates almost exactly the robustness and EAL levels delineated in the IATF.

Determining the Evaluation Assurance Level

In general, once the MAC of the information system has been determined, the IA control found in the appropriate attachment of DoDI 8500.2 indicates the level of robustness required for the solution. Then, by applying the guidance found in appendix E of the IATF or appendix H, enclosure C, of CJSCM 6510.01C, the EAL needed for the IA or IA-enabled product may be determined. Only National Information Assurance Partnership (NIAP)-validated products, configured in accordance with DoD security policy and well maintained, should be considered for incorporation into the DoD information system.

However, some circumstances may moderate robustness and resulting EAL requirements. For example, IA or IA-enabled products that protect for confidentiality could be less robust for an encrypted network because of the level of protection provided by the existence of the encryption. In the same system, products that protect for availability would still have to meet the higher robustness and EAL requirements; if the product protects for confidentiality and integrity, the higher robustness and EAL solution should prevail.

Exceptional EAL Determination Issues

Sometimes a particular configuration or scenario may require developers or integrators to assess what strength of mechanisms or levels of assurance is needed because of a specific threat environment not covered under the system's mission assurance category. For example, this situation could occur when the system in question will connect to systems of that have differing mission assurance categories.

In this case, DoDI 8500.2 addresses platform IT interconnections under one guidance paragraph and other interconnections in another paragraph. In the first case, paragraph E3.4.1.4, states that, "When platform IT interconnects with external networks in order to exchange information, the IA requirements generated by the exchange must be explicitly addressed as part of the interconnection. If not already established, as part of the interconnection negotiation, the platform shall identify the mission assurance category and confidentiality level of its interconnecting IT. The connecting enclave must meet or exceed the mission assurance category and confidentiality level of the interconnecting platform IT." As seen in this paragraph, the MAC and confidentiality of

the interconnecting system must meet the MAC and confidentiality of the platform IT to which it connects, so the robustness and EAL must meet the same requirements.

For all other interconnections, paragraph E3.4.1.2 of DoDI 8500.2 states, “An enclave's mission assurance category and security domain remain fixed during interconnection to other enclaves; they do not inflate to match the mission assurance category or security domain of an interconnecting enclave. Enclaves with higher mission assurance categories connecting to enclaves with lower mission assurance categories are responsible for ensuring that the connection does not degrade its availability or integrity...” This interconnecting boundary is where an assessment of the strength of mechanisms or levels of assurance is needed in order to ensure that the connection does not degrade the higher mission assurance category system’s availability or integrity.

This assessment is accomplished by referring to paragraph 4.5, “Robustness Strategy,” in the IATF. To determine the level of security provided by a given IA or IA-enabled product, the value of the information to be protected (the higher MAC system) and the perceived threat environment (in connecting to the lower MAC system) should be considered. Once this consideration has been made, Table 4-7, found in the IATF may be used to determine the required EALs.

This is an extract of Table 4-7 found in the IATF

Information Value	Threat Levels						
	T1	T2	T3	T4	T5	T6	T7
V1	EAL1	EAL1	EAL1	EAL2	EAL2	EAL2	EAL2
V2	EAL1	EAL1	EAL1	EAL2	EAL2	EAL3	EAL3
V3	EAL1	EAL2	EAL2	EAL3	EAL3	EAL4	EAL4
V4	EAL1	EAL2	EAL3	EAL4	EAL5	EAL5	EAL6
V5	EAL2	EAL3	EAL4	EAL5	EAL6		

Levels of information value:

• **V1.** Violation of the information protection policy would have negligible adverse effects or consequences

• **V2.** Violation of the information protection policy would adversely affect and/or cause minimal damage to the security, safety, financial posture, or infrastructure of the organization.

• **V3.** Violation of the information protection policy would cause some damage to the security, safety, financial posture, or infrastructure of the organization.

• **V4.** Violation of the information protection policy would cause serious damage to the security, safety, financial posture, or infrastructure of the organization.

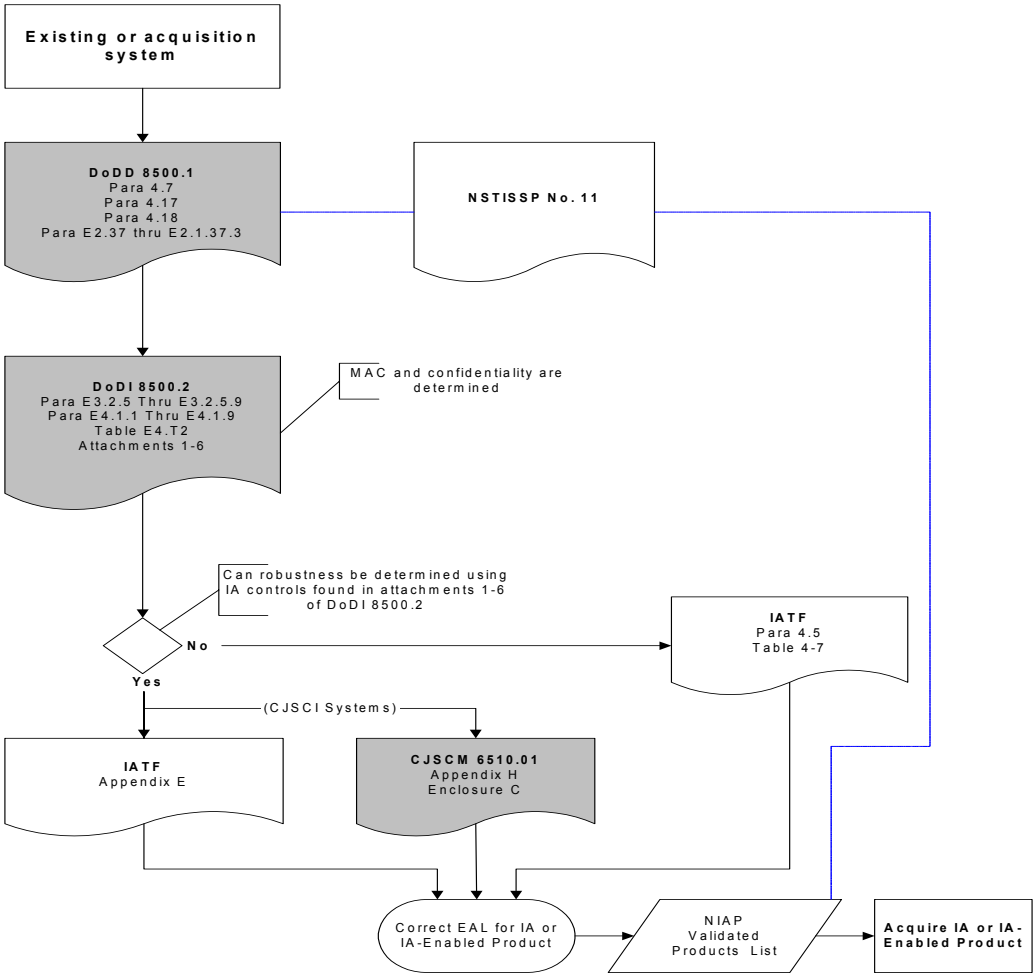
• **V5.** Violation of the information protection policy would cause exceptionally grave damage to the security, safety, financial posture, or infrastructure of the organization.

Levels of threat:

- **T1.** Inadvertent or accidental events (e.g., tripping over a power cord).
- **T2.** Passive, casual adversary with minimal resources who is willing to take little risk (e.g., listening).
- **T3.** Adversary with minimal resources who is willing to take significant risk (e.g., unsophisticated hackers).
- **T4.** Sophisticated adversary with moderate resources who is willing to take little risk (e.g., organized crime, sophisticated hackers, international corporations).
- **T5.** Sophisticated adversary with moderate resources who is willing to take significant risk (e.g., international terrorists).
- **T6.** Extremely sophisticated adversary with abundant resources who is willing to take little risk (e.g., well-funded national laboratory, nation-state, international corporation).
- **T7.** Extremely sophisticated adversary with abundant resources who is willing to take extreme risk (e.g., nation-states in time of crisis).

Process Flow Schema

The schematic below describes the correlation and workflow process used to establish the evaluation assurance level of the IA or IA-enabled solution based the mission assurance category of the system and any systems that may be inter-connected.



Summary

As can be seen from the documentation presented, there is a correlation between robustness, found both in the IA controls delineated in 8500.2 and the engineering processes described in the IATF, that helps determine the appropriate assurance level of IA or IA-enabled products. However, that correlation is tenuous in that the definition of robustness is broad and the array of other possible solutions that may be implemented, technically, non-technically, and in policy, is rather large.

Prior to selecting IA or IA-enabled products, IA engineers should look carefully at the Common Criteria (CC) product's security target, and, if one exists, the protection profile, to ascertain the appropriate assurance level the product should deliver for integrity or confidentiality of the information that is being protected.

Remember, choosing the correct IA or IA-enabled product with appropriate EAL is part of the DoD defense-in-depth, a layered defense solution that should be deployed across the DoD enterprise.

References

a. DoD Directive 8500.1, “Information Assurance (IA),” 24 October 2002

b. DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” 6 February 2003

c. Chairman Joint Chiefs of Staff Manual 6510.01 (CJCSM), “Defense-In-Depth, Information Assurance and Computer Network Defense (CND),” 25 March 2003

d. Information Assurance Technical Framework, release 3.1, September 2002

e. The National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-enabled Information Technology Products," Revised Fact Sheet July 2003

f. Frequently Asked Questions: DoDI 8500.2, 20 March 2003